QSC 18 | QUALYS SECURITY CONFERENCE 2018

Web Applications & APIs

Application Security in a Devops world

Pierrick Prevert
Security Solutions Architect

Remi Le Mer
Director of Product Management, WAF

Agenda

Web Applications & APIs: where are we now ?

Web Security Built-in, not bolted on

Qualys Web Application Scanning

Review | What's New | Roadmap

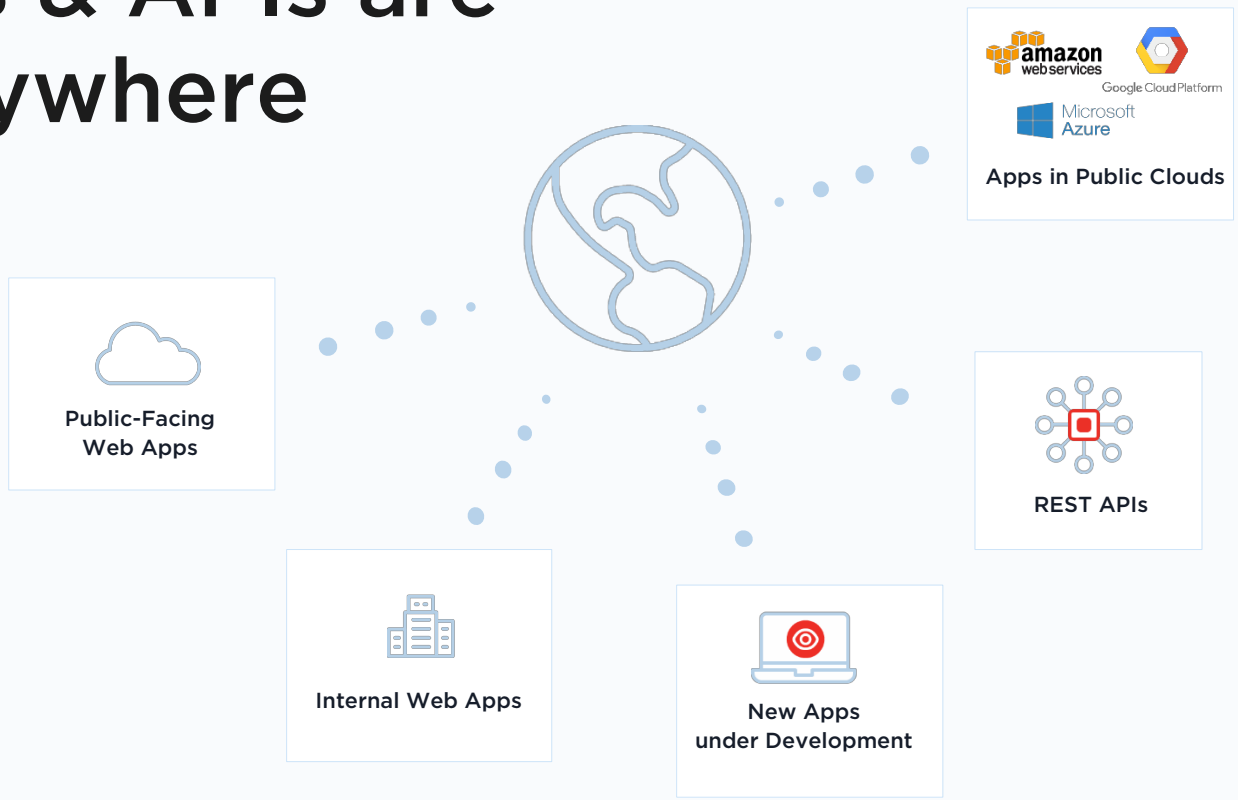
Qualys Web Application Firewall

Review | What's New | Roadmap

Bug Bounty, a new horizon ?

Q&A

Apps & APIs are Everywhere



Insecure Apps & APIs are a Problem

Business depends on web applications

Any of them can be a foothold into your organization

Developers are not incentivized for security

Cloud-based apps are easy for developers to deploy

Web Applications are Being Targeted

- Most common data breach pattern *
- Top hacking vector *

U.S. Postal Service (API)	2018
Facebook (API)	2018
Google+ (API)	2018
MyFitnessPal (API?)	2017
Equifax	2017
Yahoo	2016
Ashley Madison	2015

*** Source: 2018 Verizon DBIR**

Devops challenges how security is done

Security should start in dev

Security should be a continuous effort

Security is a global concern

CI/CD Tools are powerful

New challenges:

What is in production ?

What server is this app on ?

CI/CD pipe's privileges ?

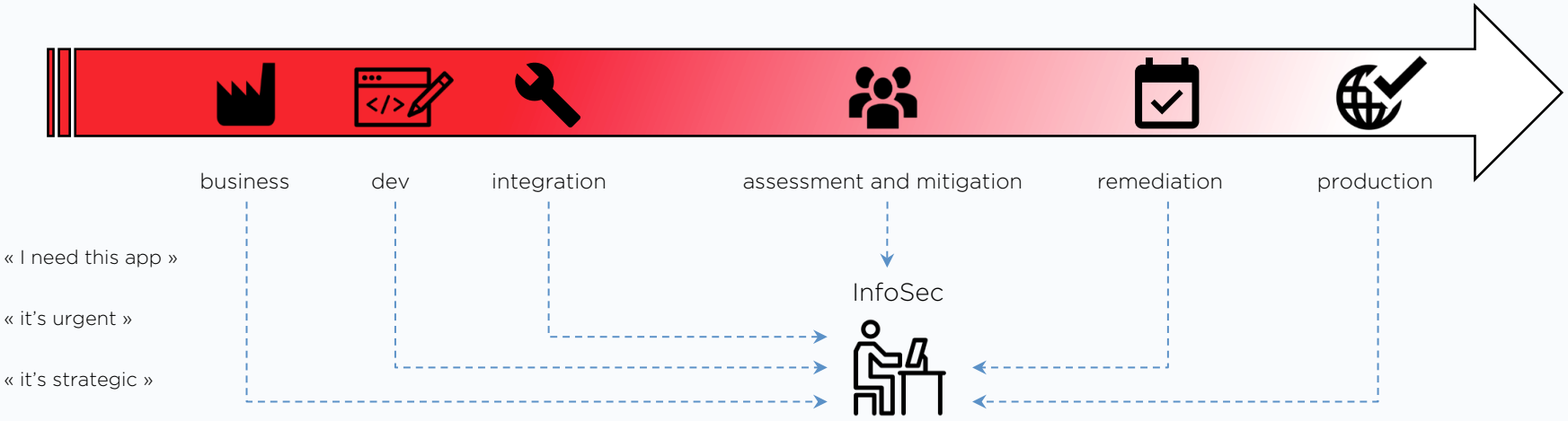
Inefficient/late security

Slowed-down delivery

Web Application Security Built-in

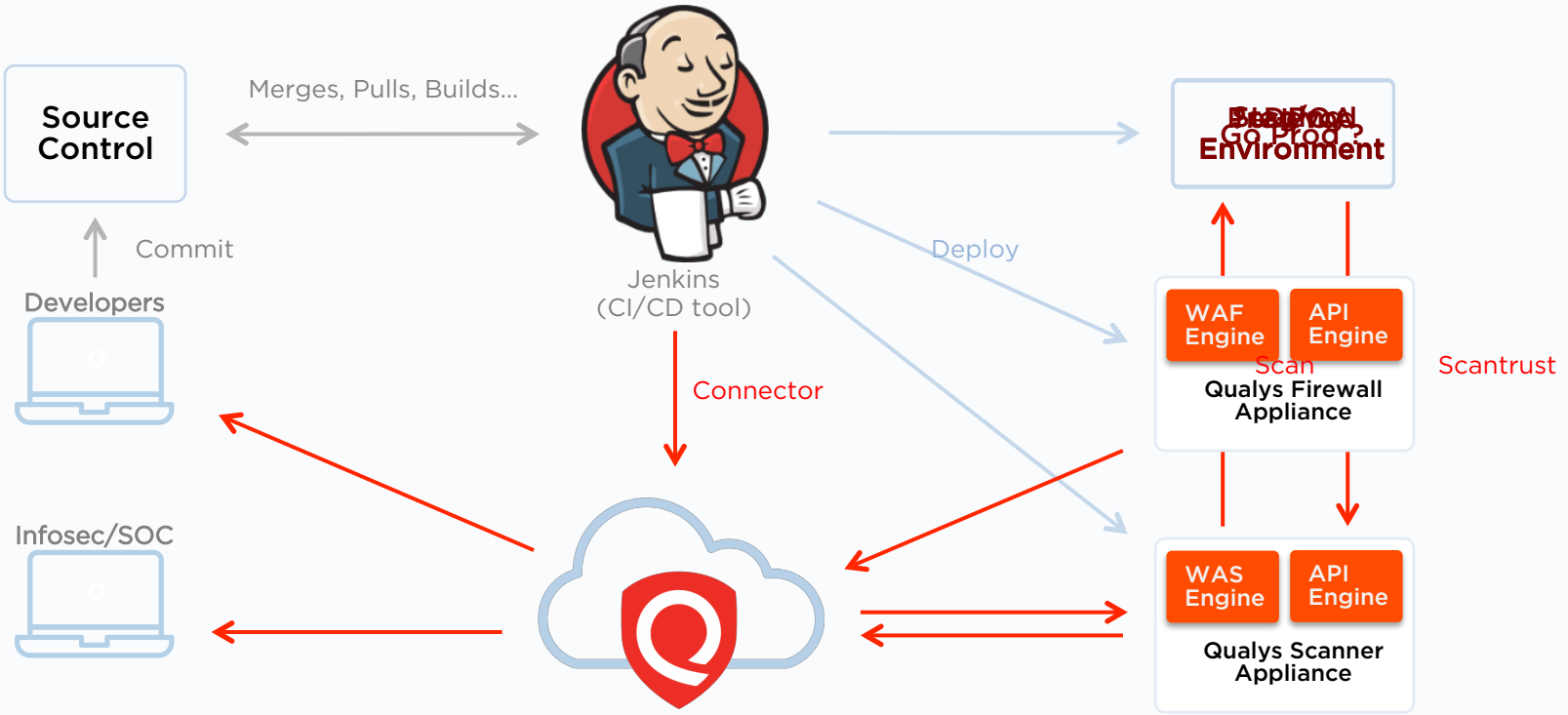
...Not bolted on

Traditional AppSec Operations



Qualys.

The way of the DevSecOps

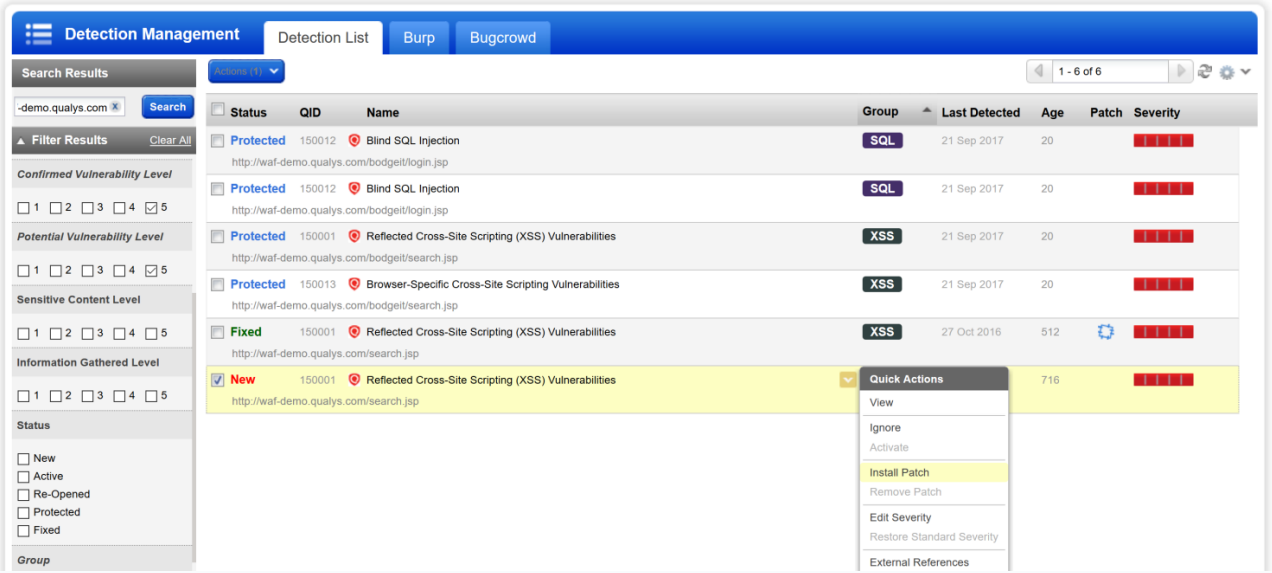


Qualys.

WAS / WAF Integration: ScanTrust

ScanTrust : Challenge your WAF protection

Assess both the application and the policy that protects it

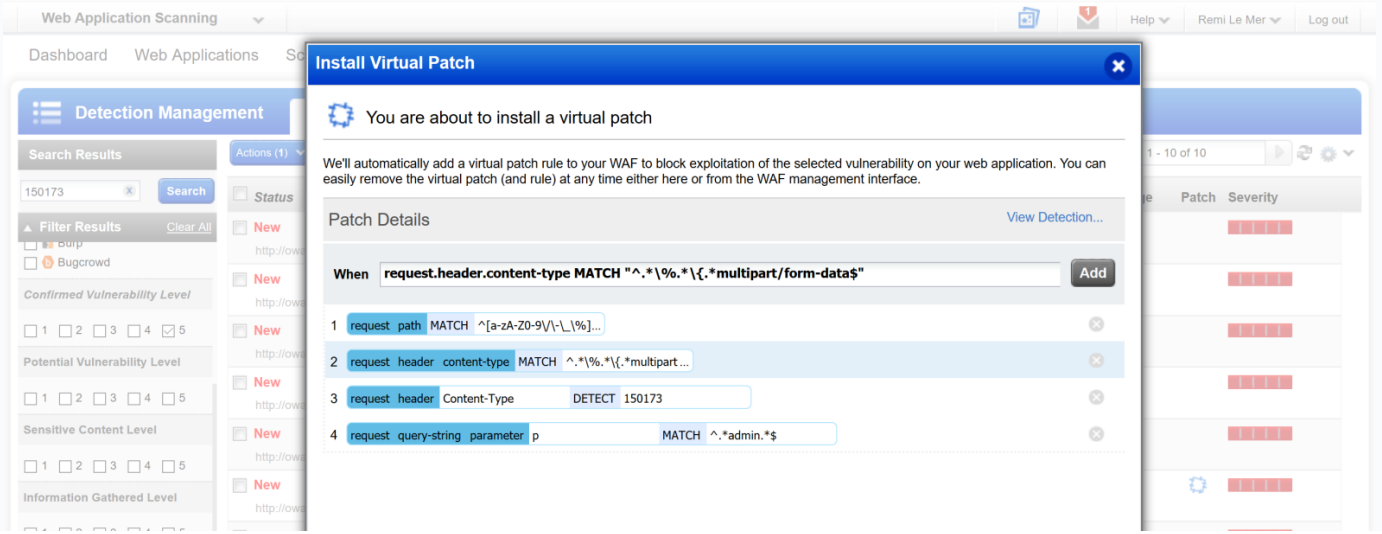


Qualys.

WAS / WAF Integration: Virtual Patch

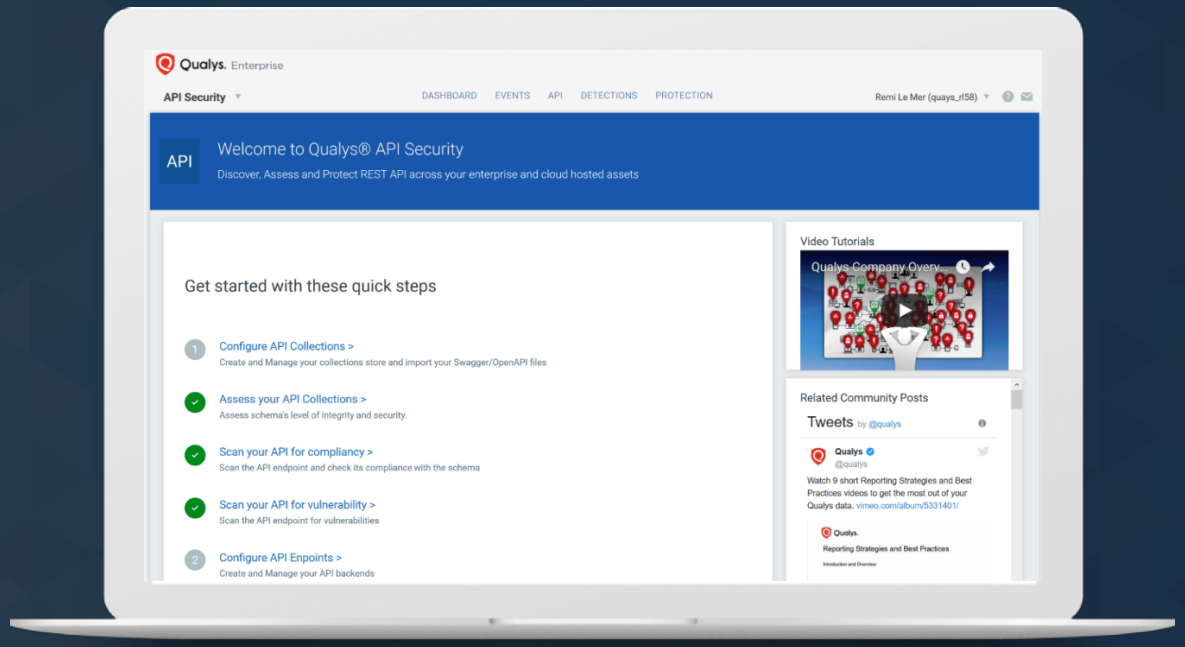
Virtual Patch : One-click mitigation tool for CISO teams

Run from within WAS to address confirmed threats



Qualys.

And Coming in 2019



Web Application Scanning

Review

Qualys WAS

A leading dynamic application security testing (DAST) tool

Delivered via the Qualys Cloud Platform

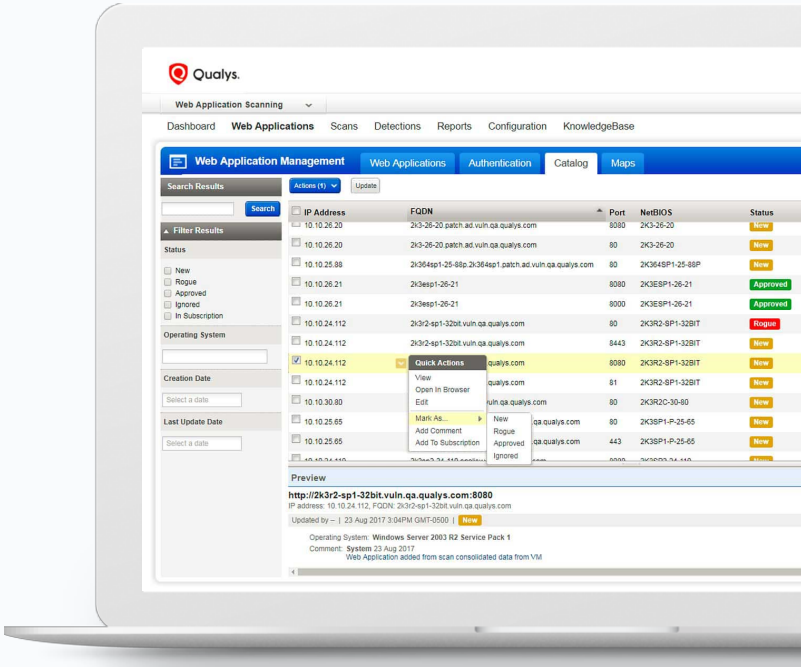
Identifies app-layer vulnerabilities

- OWASP Top 10
- CWEs
- Web-related CVEs

Includes automated crawling

Supports Selenium scripts

Malware monitoring as a bonus



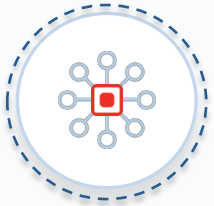
Qualys.

Built for the Enterprise

Web App Discovery
Unlimited scans & users
RBAC
Tagging

Scheduled scans
Ad-hoc, targeted scans
Multi-site scans
Retest vulnerability
Scan for malware

Massive scalability
Detection history
Scheduled reports
Customizable reports
Swagger support



Robust API
CI/CD integration
Unique integration w/Qualys WAF
Integration with manual pen testing tools

What's New in Qualys WAS

Scanning REST APIs

https://
swagger.io

https://
www.openapis.org

Swagger is specification that describes a set of REST APIs

Swagger file typically available from dev team

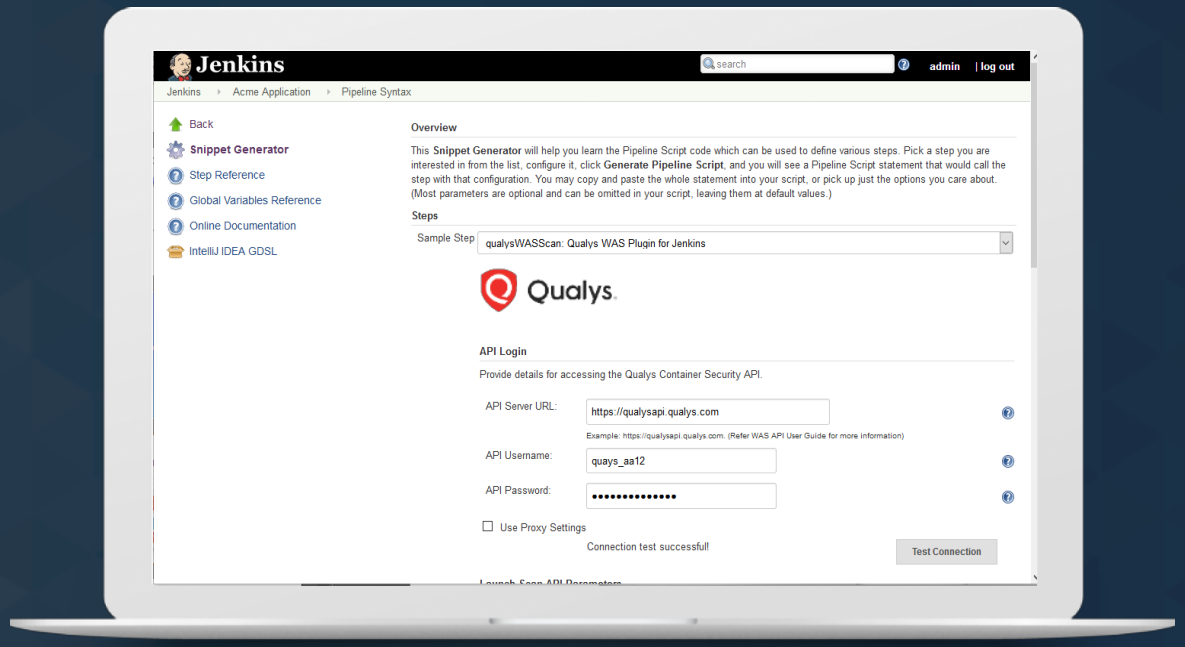
Set Swagger file as target URL in Qualys WAS

API endpoints are automatically tested for vulnerabilities

Swagger v2 JSON format currently supported

Qualys

Jenkins Plugin for WAS



Manual Testing Complements WAS

Dynamic application testing is one piece of the AppSec puzzle

Manual penetration testing important for your business-critical apps

Qualys WAS offers:

- Bugcrowd integration
- Burp Suite integration
- Partnerships with consulting shops

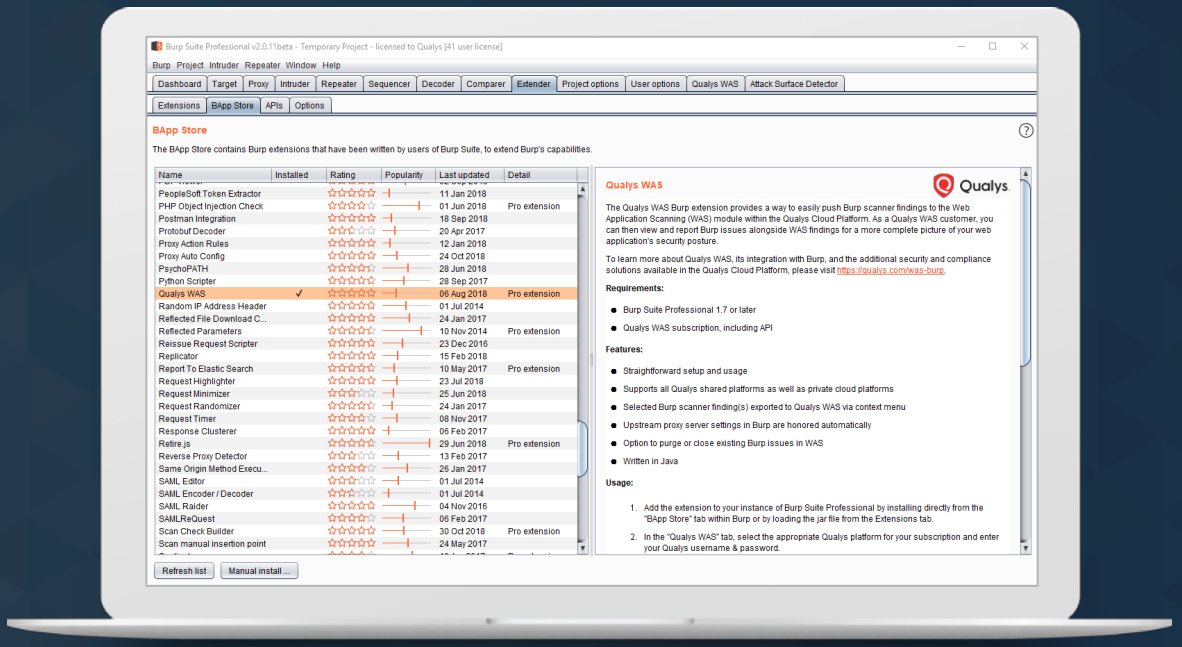
Bi-directional Integration with Bugcrowd

Qualys WAS Burp Extension

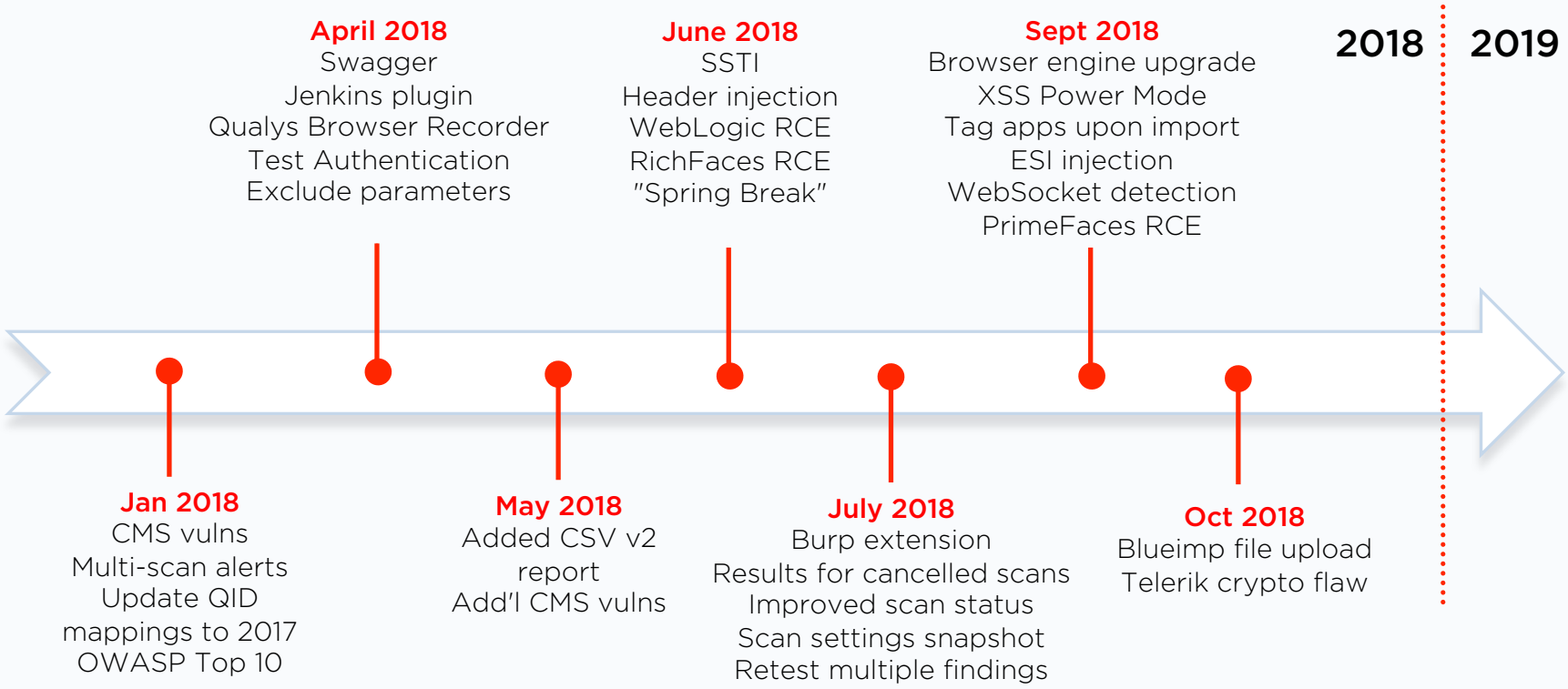
A quick, intuitive way to send Burp-discovered issues into WAS
Provides centralized viewing/reporting of WAS detections + Burp issues

Available in Burp's BApp Store

Qualys WAS Burp extension



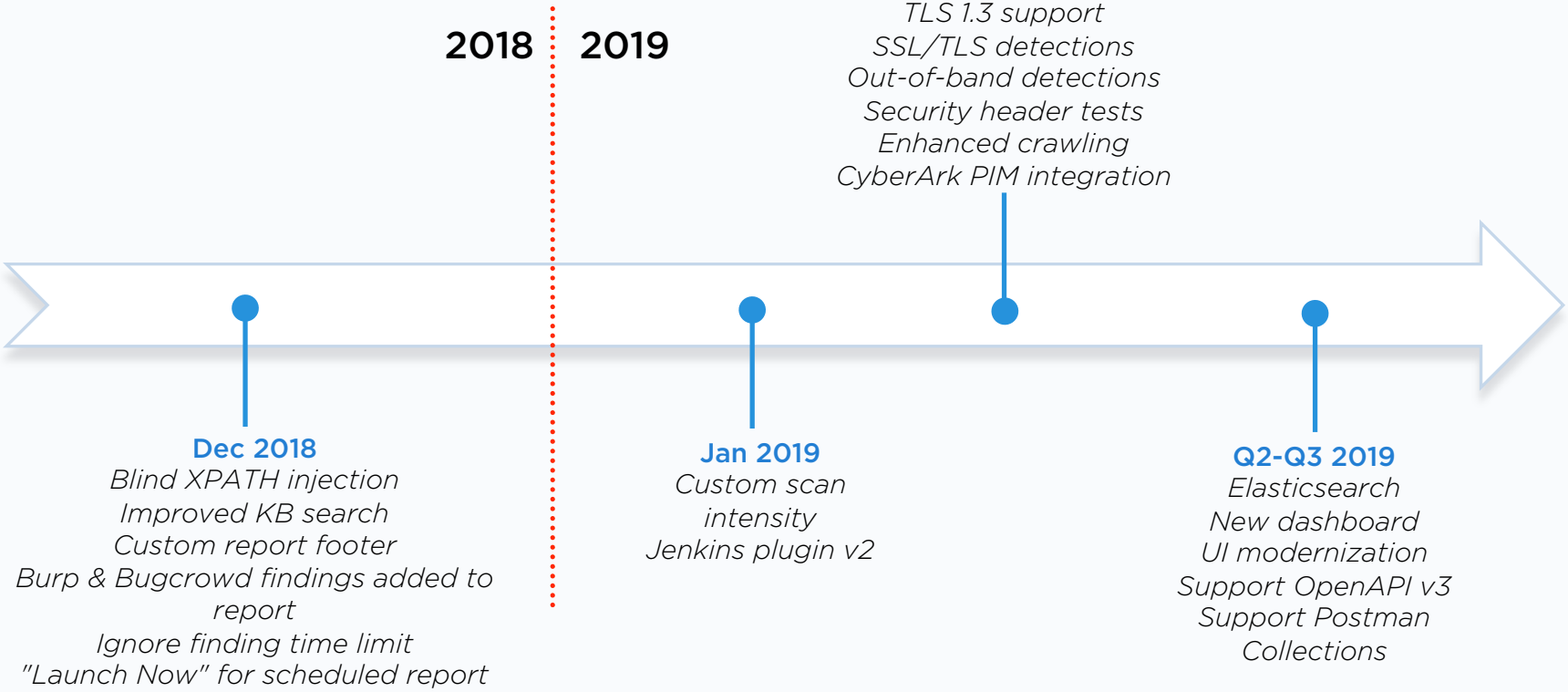
WAS Enhancements, YTD



Qualys.

Qualys WAS Roadmap

WAS Roadmap



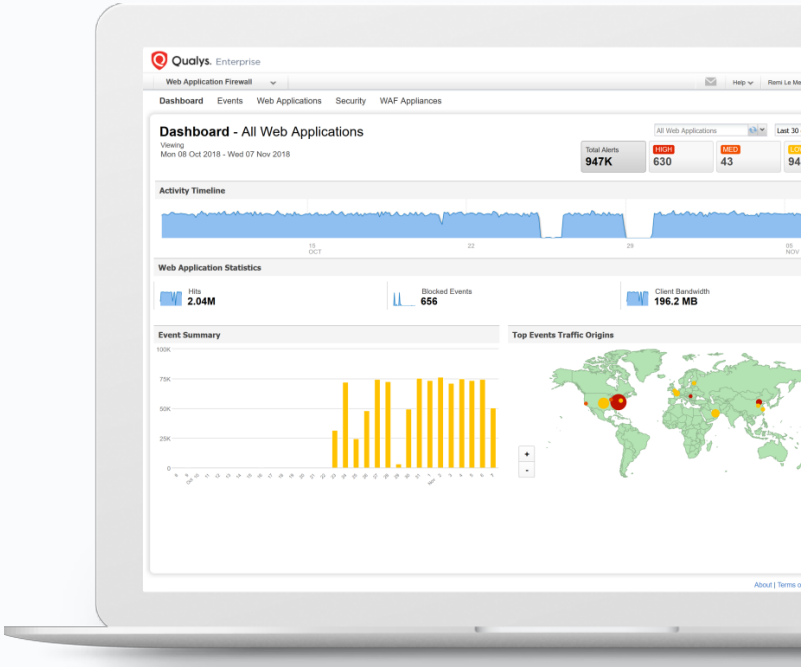
Qualys.

Web Application Firewall

Review

Qualys WAF

Integration with WAS
Architecture improvements
Integration with Docker
Security Improvements
Roadmap – standalone
Roadmap – Integrated Suite



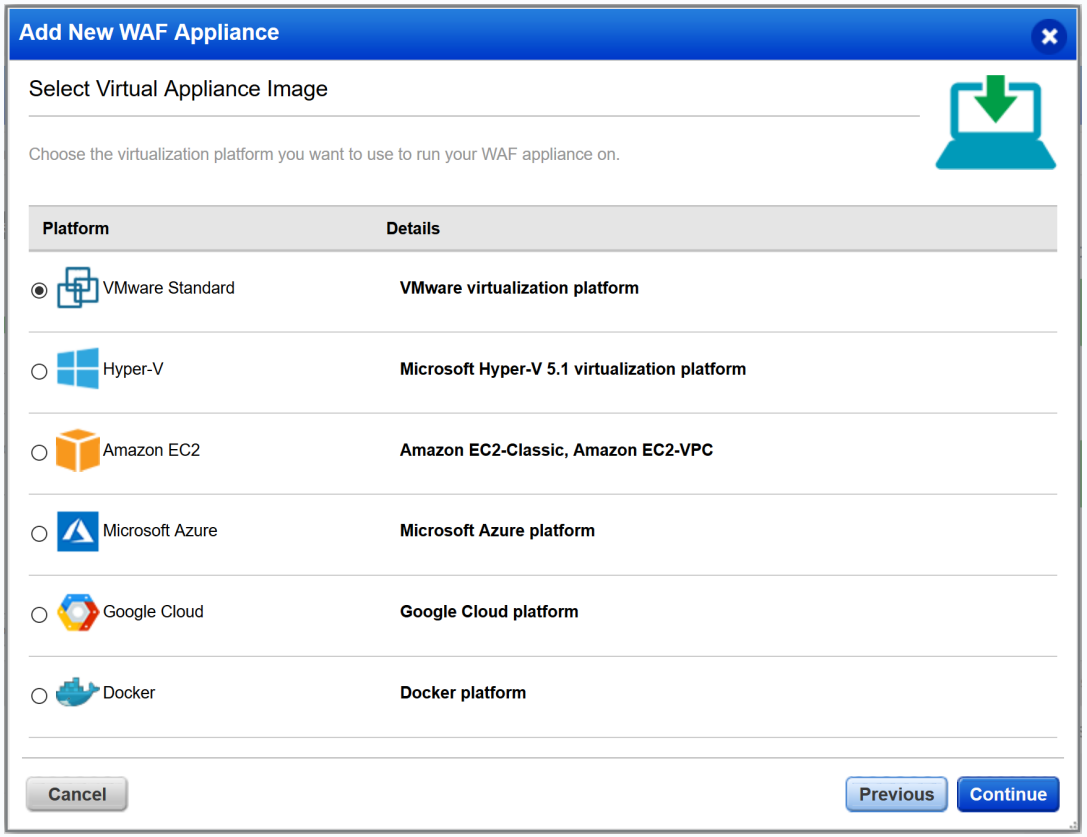
Qualys.

What's New in Qualys WAF

Supported Platforms

Shared and Private

Qualys Cloud Platforms



Qualys.

WAF Virtual Appliance

Easy and usable Architecture

- Virtual Reverse-Proxy
- Cluster-able within hybrid topologies
- Load-Balancing capabilities
- SSL/TLS cipher suite categories

WAF Improvements

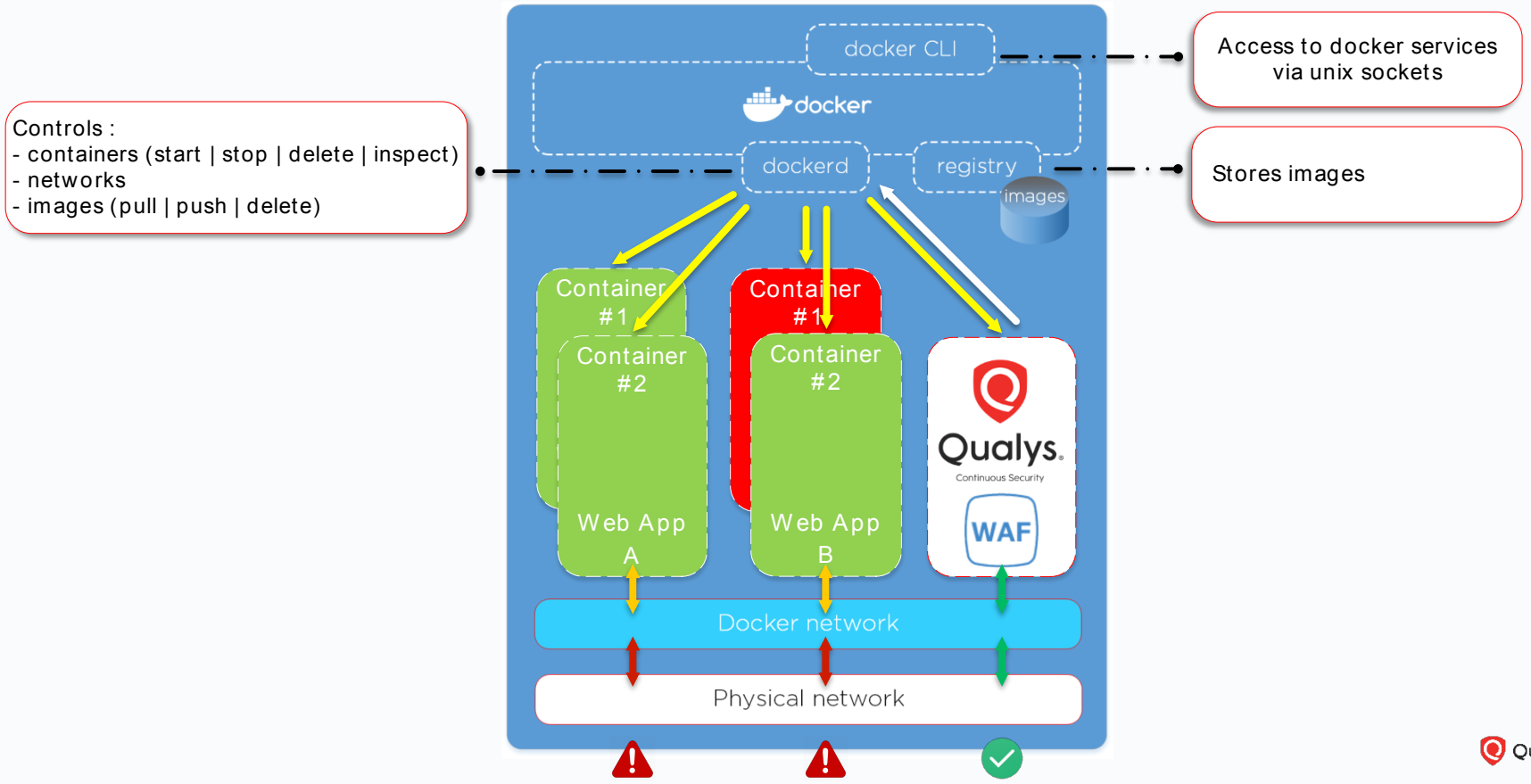
Virtual Appliance & Container (v1.5.3)

- XML/JSON content inspection
- Docker Host integration for backend automation
- Better performance
- Scheduled upgrades

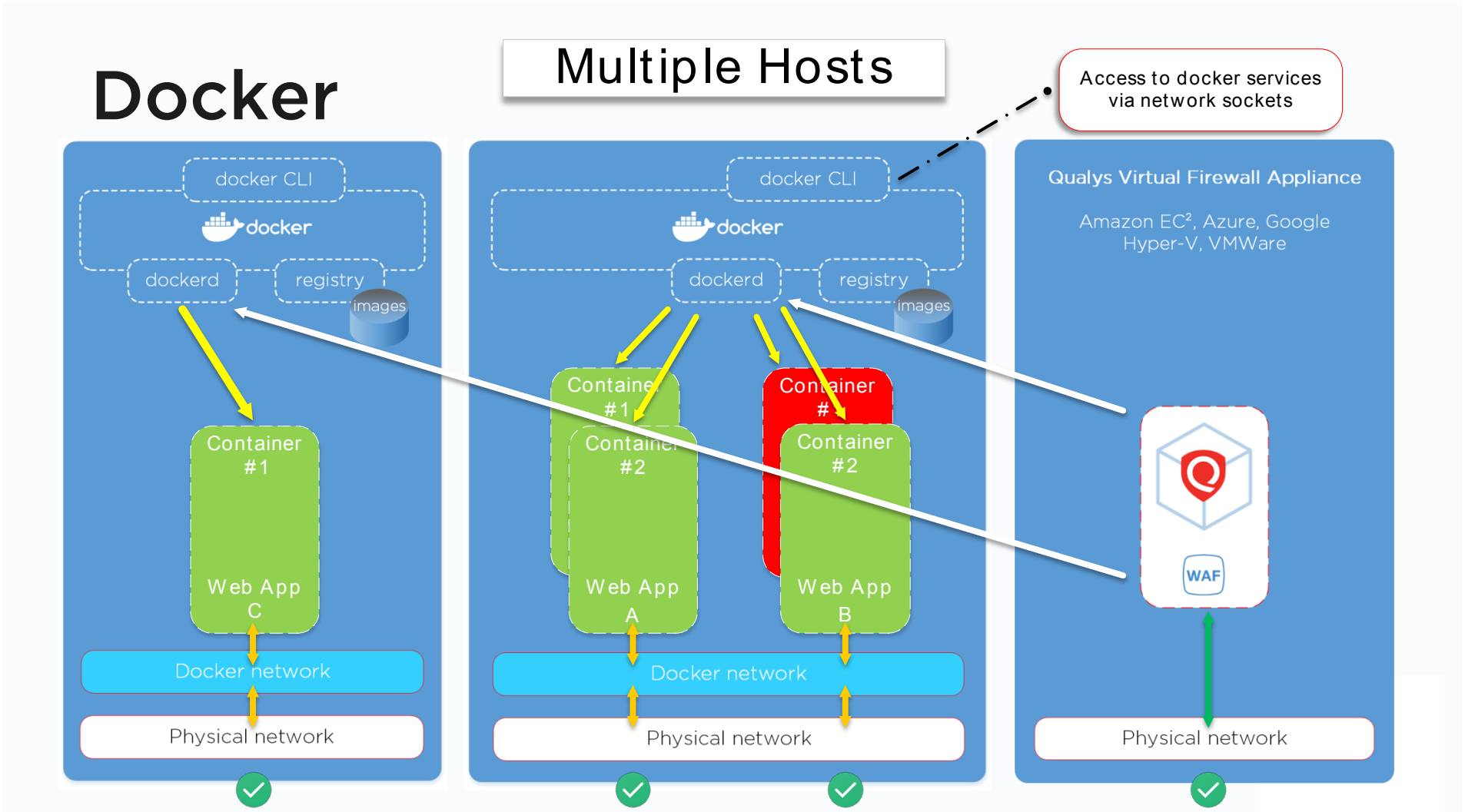
Orchestration via Qualys API

Docker

Single Host



Qualys.


Docker
Multiple Hosts
Access to docker services via network sockets
docker CLI
docker
dockerd
registry
images
Container #1
Web App C
Docker network
Physical network
docker CLI
docker
dockerd
registry
images
Container #1
Container #2
Web App A
Container #
Container #2
Web App B
Docker network
Physical network
Qualys Virtual Firewall Appliance
Amazon EC², Azure, Google Hyper-V, VMWare
WAF
Physical network

Security Improvements

Custom Rules: write and manage your own filters

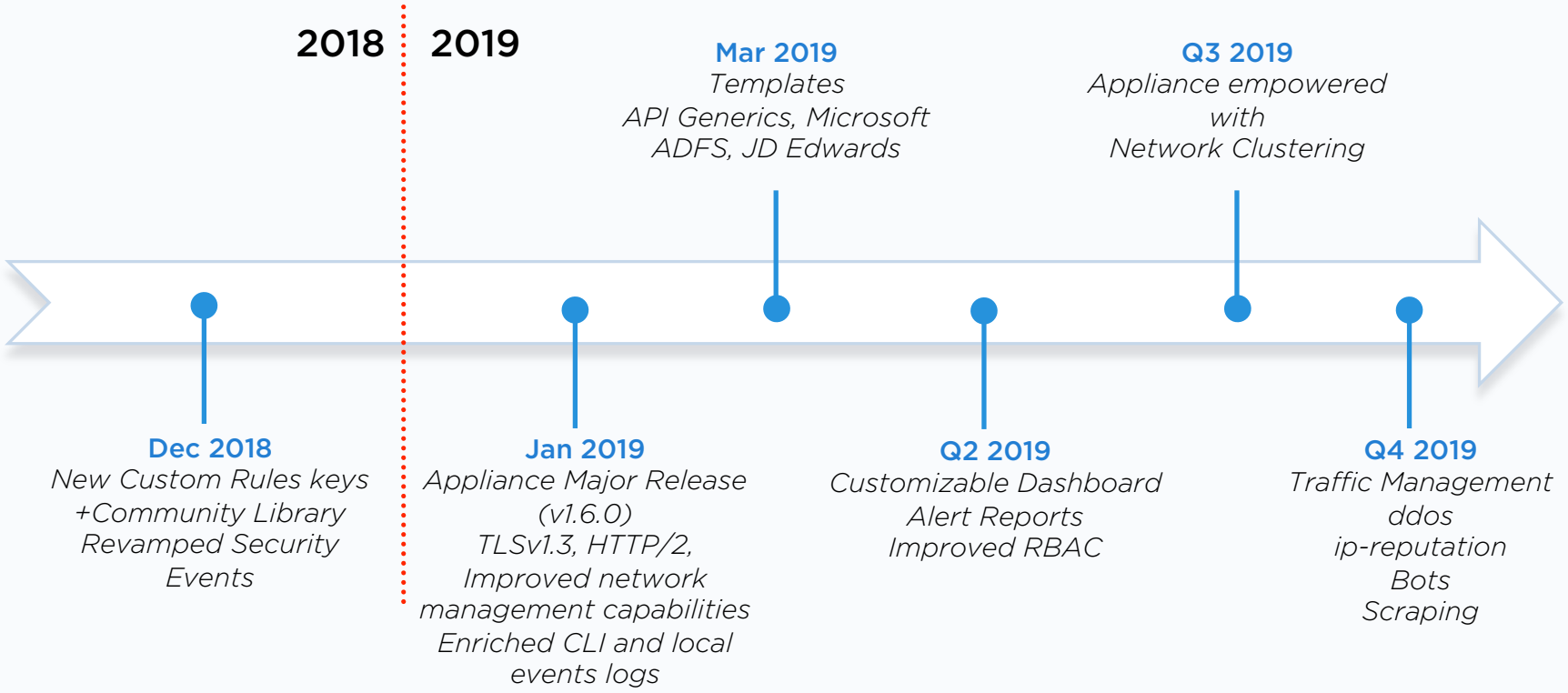
- XML/JSON inspection
- Virtual Patches and Event Exceptions
- Latency control
- Rewriting capabilities (headers)

Qualys Rulesets and Templates

- DAG based inspection, programmable logic
- Drupal 8.0.x, Joomla 3.4.x, Magento 2.5-2.6, Wordpress 4.2.x-4.3.x
- JBoss 4.x-7.x, OWA 2010-2017, Sharepoint 2010-2017, Tomcat 8.0.x
- Qualys Generics for unknown apps

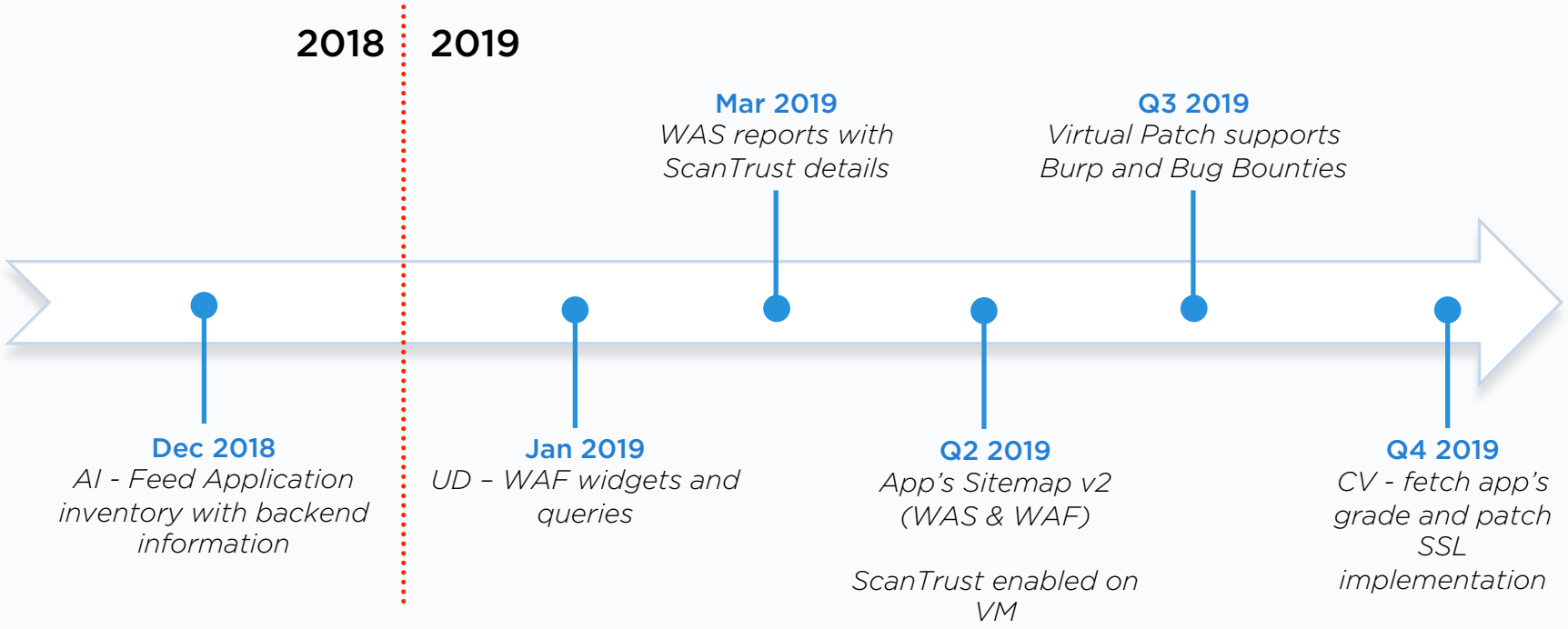
Qualys WAF Roadmap

WAF Roadmap - Standalone



Qualys.

WAF Roadmap – Integrated Suite



Qualys.

Web Applications & APIs

Intégration et capitalisation des données issues d'un programme de Bug Bounty

YES WE HACK

Romain Lecoeuvre
Co-Fondateur & CTO

Qualys.

Un peu d'histoire...

Le principe du Bug Bounty remonte à 1983, développé à partir de 1995 par Netscape pour permettre à une organisation d'améliorer la sécurité de son système d'information en s'appuyant sur une communauté de chercheurs en vulnérabilités (Crowdsecurity).

Get a bug if you find a bug.

Show us a bug in our VRTX® real-time operating system and we'll return the favor. With a bug of your own to show off in your driveway.

There's a catch, though.

Since VRTX is the only microprocessor operating system completely sealed in silicon, finding a bug won't be easy.

Because along with task management and communication, memory management, and character I/O, VRTX contains over 100,000 man-hours of design and testing.

And since it's delivered in 4K bytes of ROM, VRTX will perform for you the way it's performing in hundreds of real-time applications from avionics to video games.

Bug free.

So, to save up to 12 months of development time, and maybe save a loveable little car from the junkyard, contact us. Call (415) 326-2950, or write Hunter & Ready, Inc., 445 Sherman Avenue, Palo Alto, California 94306.

Describe your application and the microprocessors you're using—Z8000, Z80, 68000, or 8086 family. We'll send you a VRTX evaluation package, including timings for system calls and interrupts. And when you order a VRTX system for your application, we'll include instructions for reporting errors.*

But don't feel bad if in a year from now there isn't a bug in your driveway.

There isn't one in your operating system either.

HUNTER & READY

VRTX

Operating Systems in Silicon.

*Call or write for details. But, considering our taste in cars, you might want to accept our offer of $1,000 cash instead. © 1983 Hunter & Ready, Inc.

YesWeHack en chiffres

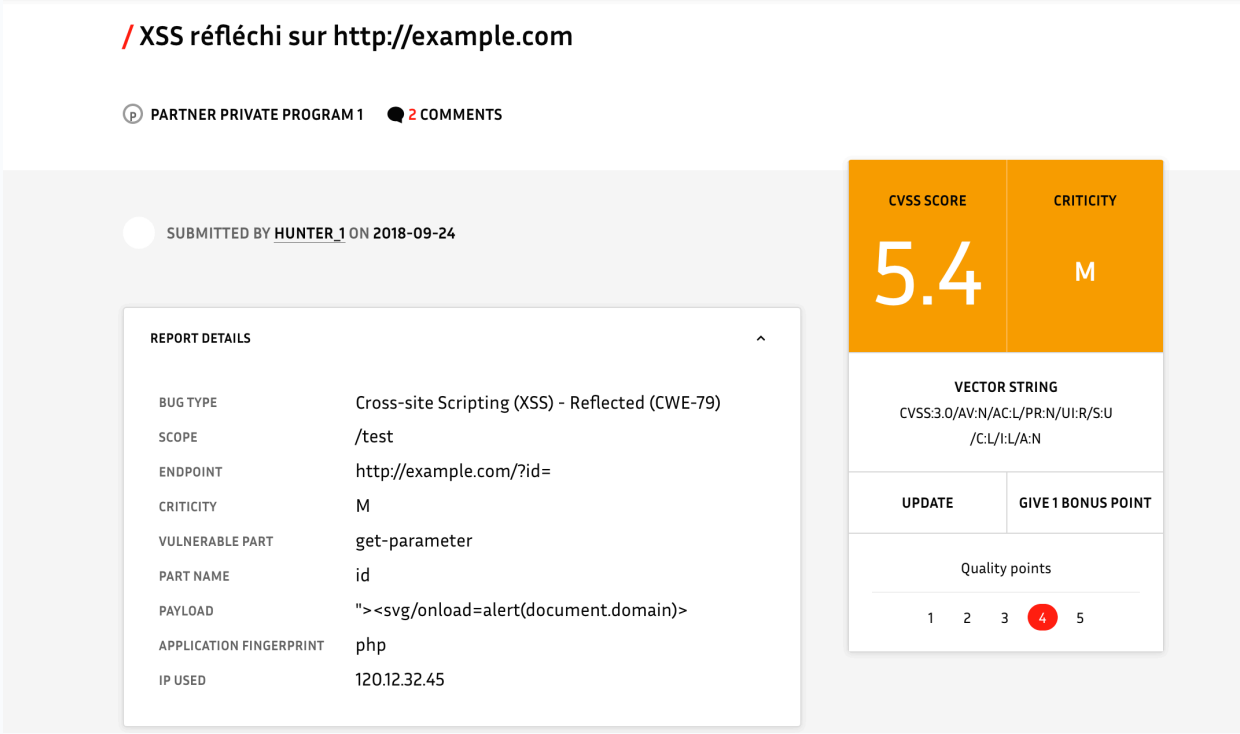
6000+ chercheurs inscrits

120+ nationalités

65% d'Européens

5500+ rapports de vulnérabilités

Structure d’un rapport

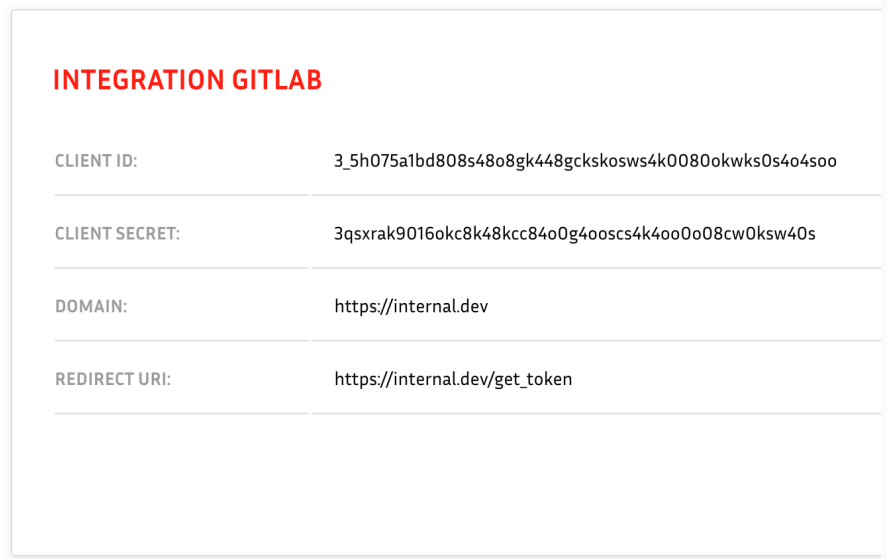


Qualys.

Intégration ?

Récupération des nouveaux rapports de vulnérabilités via API

Intégration des rapports qualifiés dans un Bug Tracker (Bitbucket, git, jira, etc.)



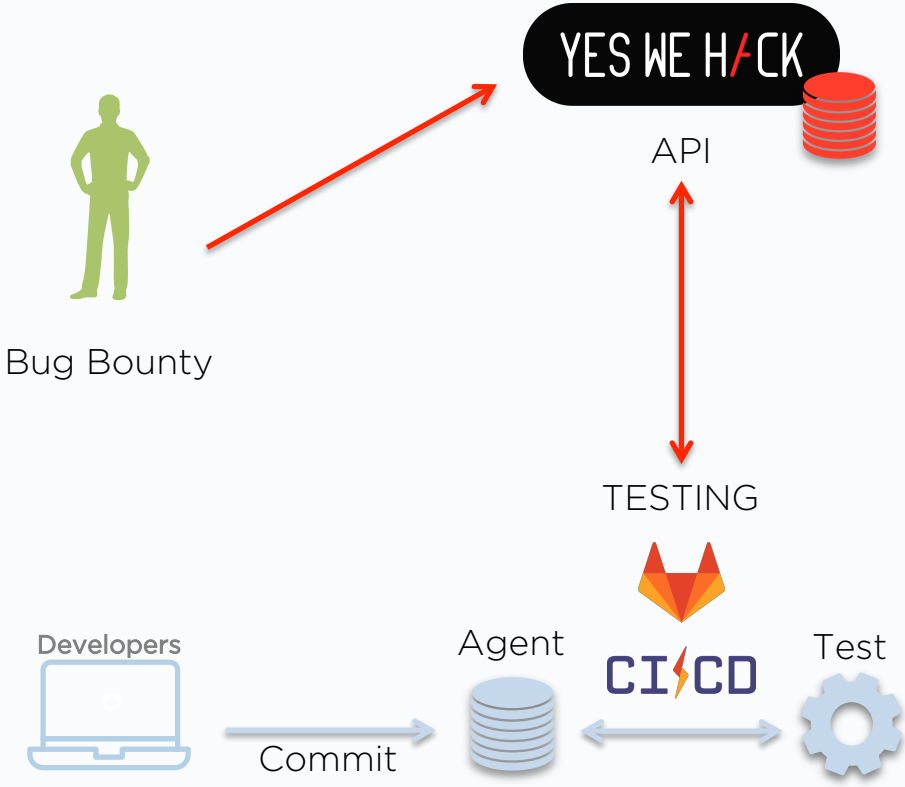
Intégration ?

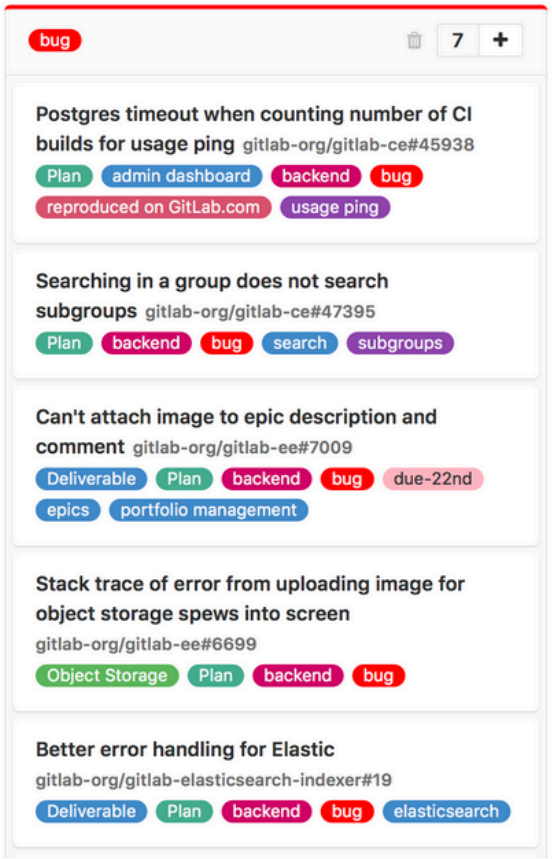
Agent de contrôle intégré dans la CI

Contrôle entre les rapports de vulnérabilités valides et les tests fonctionnels « sécurité »

Non-regression

Capitalisation ?



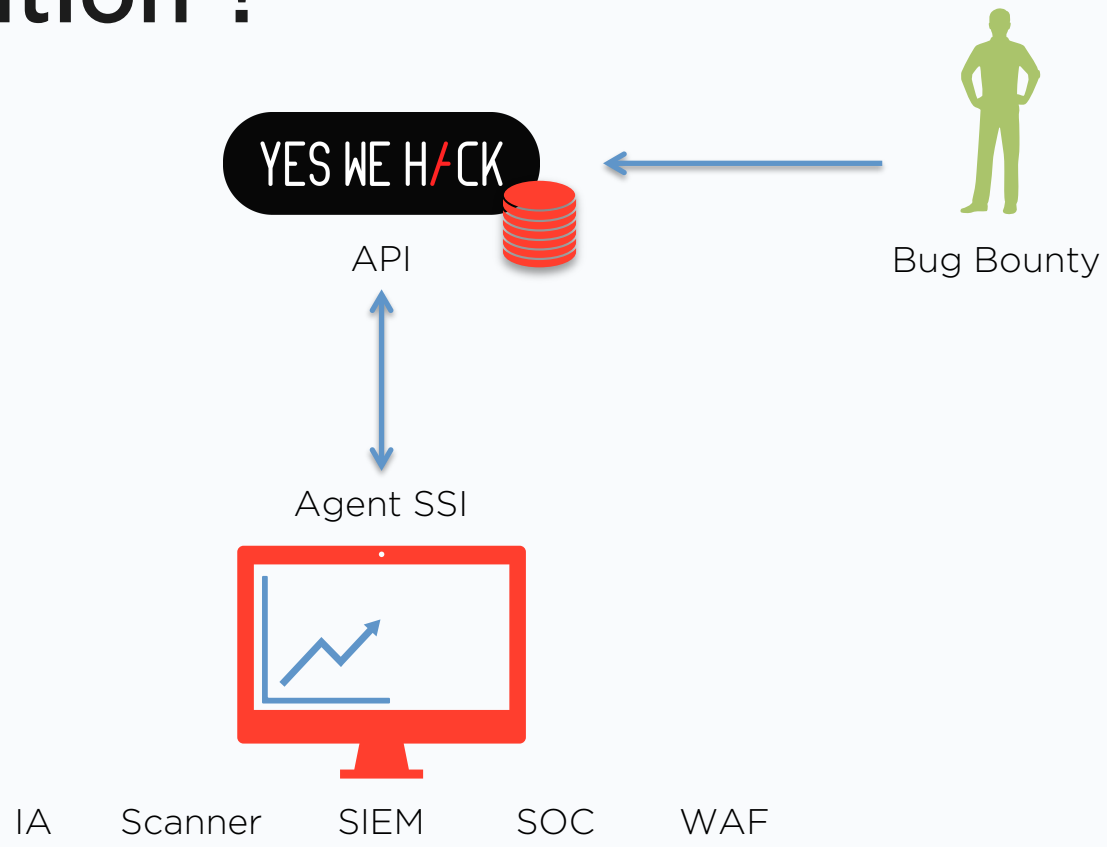


Capitalisation ?

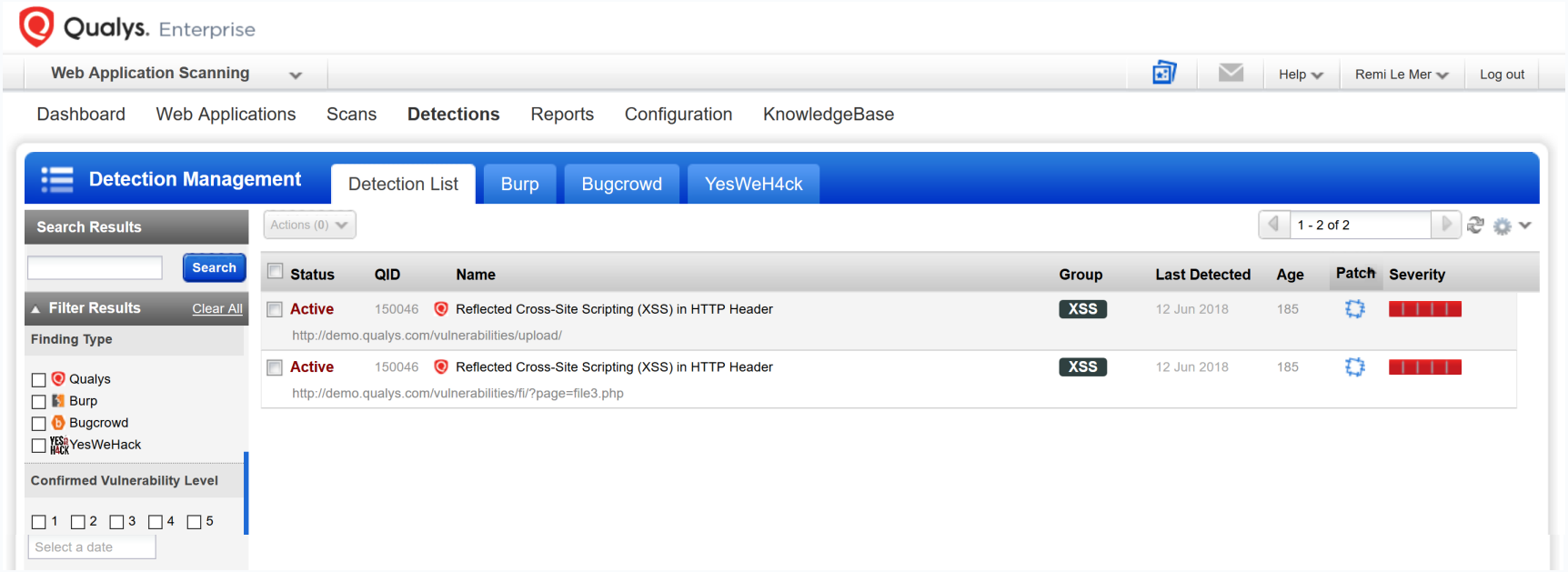
Agent intégré dans les applications métiers

- IA
- Scanner
- SIEM
- SOC
- WAF

Capitalisation ?



Capitalisation ?



Q&A

Qualys.

Thank You

Romain Lecoeuvre - rlecoeuvre@yeswehack.com
Pierrick Prevert - pprevert@qualys.com
Remi Le Mer - rlemer@qualys.com